

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2005/017305

International filing date: 20 September 2005 (20.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-308554
Filing date: 22 October 2004 (22.10.2004)

Date of receipt at the International Bureau: 28 October 2005 (28.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 1 0 月 2 2 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 3 0 8 5 5 4

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 3 0 8 5 5 4

出 願 人
Applicant(s): 日 本 電 信 電 話 株 式 有 限 公 司

2 0 0 5 年 1 0 月 1 2 日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



【書類名】	特許願
【整理番号】	NTTH166078
【提出日】	平成16年10月22日
【あて先】	特許庁長官殿
【国際特許分類】	H04L 12/46
【発明者】	
【住所又は居所】	東京都千代田区大手町二丁目3番1号
【氏名】	日本電信電話株式会社内 瀬林 克啓
【発明者】	
【住所又は居所】	東京都千代田区大手町二丁目3番1号
【氏名】	日本電信電話株式会社内 倉上 弘
【発明者】	
【住所又は居所】	東京都千代田区大手町二丁目3番1号
【氏名】	日本電信電話株式会社内 副島 裕司
【発明者】	
【住所又は居所】	東京都千代田区大手町二丁目3番1号
【氏名】	日本電信電話株式会社内 エリック チェン
【発明者】	
【住所又は居所】	東京都千代田区大手町二丁目3番1号
【氏名】	日本電信電話株式会社内 富士 仁
【特許出願人】	
【識別番号】	000004226
【氏名又は名称】	日本電信電話株式会社
【代理人】	
【識別番号】	100089118
【弁理士】	
【氏名又は名称】	酒井 宏明
【選任した代理人】	
【識別番号】	100114306
【弁理士】	
【氏名又は名称】	中辻 史郎
【手数料の表示】	
【予納台帳番号】	036711
【納付金額】	16,000円
【提出物件の目録】	
【物件名】	特許請求の範囲 1
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1
【包括委任状番号】	0310351

【書類名】 特許請求の範囲

【請求項 1】

パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置であって、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、

前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、

を備えたことを特徴とする中継装置。

【請求項 2】

前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、

前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、

前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項 1 に記載の中継装置。

【請求項 3】

攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手段を備え、

当該シグネチャ生成手段は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項 2 に記載の中継装置。

【請求項 4】

前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を他の隣接中継装置に送信するとともに、当該シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、当該シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報および容疑シグネチャを前記シグネチャ記憶手段に対応付けて登録し、

前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されている場合には、当該生成識別情報に対応付けて登録されている中継元情報が前記受信したシグネチャの中継元情報と同一であるか否かをさらに判定し、

前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に既に登録されているが、前記中継元情報が同一であると判定された場合には、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に上書き登録するとともに、当該シグネチャを前記シグネチャ記憶手段に登録されている中継先情報が示す他の隣接中継装置に送信することを特徴とする請求項 3 に記載の中継装置。

【請求項 5】

前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記中継元情報が同一でないと判定された場合には、前記シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送し、さらに、当該既登録通知を他の隣接中継装置から受信した場合には、前記シグネチャ記憶手段に記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除することを特徴とする請求項

4 に記載の中継装置。

【請求項 6】

パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、

前記中継装置は、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、

前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、

を備えたことを特徴とするネットワーク攻撃防御システム。

【請求項 7】

パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継方法であって、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定工程と、

前記識別情報判定工程によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信工程と、

を含んだことを特徴とする中継方法。

【請求項 8】

前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、

前記シグネチャ登録判定工程は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、

前記シグネチャ通信工程は、前記シグネチャ登録判定工程によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項 7 に記載の中継方法。

【請求項 9】

攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成工程を含み、

当該シグネチャ生成工程は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項 8 に記載の中継方法。

【請求項 10】

パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、

前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手順と、

前記識別情報判定手順によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手順と、

をコンピュータに実行させることを特徴とする中継プログラム。

【請求項 1 1】

前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、

前記シグネチャ登録判定手順は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、

前記シグネチャ通信手順は、前記シグネチャ登録判定手順によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする請求項 1 0 に記載の中継プログラム。

【請求項 1 2】

攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手順をコンピュータに実行させ、

当該シグネチャ生成手順は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする請求項 1 1 に記載の中継プログラム。

【書類名】 明細書

【発明の名称】 中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システム

【技術分野】

【0001】

この発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャリストに登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムに関する。

【背景技術】

【0002】

従来より、防御対象であるコンピュータが接続されたネットワーク上に複数の中継装置を有し、D o S (Denial of Service) 攻撃またはD D o S (Distributed Denial of Service) 攻撃を受けるコンピュータを防御するネットワーク攻撃防御システムが知られている。例えば、特許文献1 (特開2003-283554号公報) や特許文献2 (特開2003-283572号公報) に開示されたネットワーク攻撃防御システムでは、中継装置において、予め決められた攻撃容疑パケットの検出条件に通信トラヒックが合致するか否かをチェックする。そして、合致したトラヒックを検出した場合に、中継装置は、検出された攻撃容疑パケットの伝送帯域制限値を表すシグネチャを生成して隣接中継装置 (隣接関係をもつ中継装置) へ送信するとともに、以後、シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行う。

【0003】

一方、シグネチャを受信した中継装置 (隣接中継装置) では、通過するパケットの伝送帯域をシグネチャによって表される伝送帯域制限値に制限するとともに、さらに上流の隣接中継装置に対してシグネチャを送信する。つまり、シグネチャを受信した各中継装置がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置が同様のシグネチャに基づいてパケットを処理し、これによって、各中継装置を通過するパケットの伝送帯域をシグネチャが示す伝送帯域制限値に制限する。なお、上流または下流の中継装置とは、隣接中継装置であり、かつ攻撃容疑パケットが流入する方向に対する中継装置である。

【0004】

さらに、一定時間経過後、攻撃を検出した中継装置は、各隣接中継装置から攻撃容疑パケットの平均入力伝送帯域値を受信し、各隣接中継装置における平均入力伝送帯域の比率により伝送帯域制限調整値を算出し、算出した伝送帯域制限調整値を隣接中継装置に送信する。そして、かかる伝送帯域制限調整値を受信した中継装置は、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整しながら、さらに上流の隣接中継装置に伝送帯域制限調整値を送信する。つまり、伝送帯域制限調整値を受信した各中継装置が伝送帯域制限調整値の送信を繰り返すことで、ネットワーク上の全ての中継装置が同様の伝送帯域制限調整値を受信し、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整する。

【0005】

【特許文献1】 特開2003-283554号公報

【特許文献2】 特開2003-283572号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

ところで、上記した従来の技術は、隣接中継装置にシグネチャを送信するので、ネットワーク攻撃防御システムにおける互いの中継装置の隣接関係によっては、異なる隣接中継装置から同一のシグネチャを受信する中継装置が存在することがある。そして、このような中継装置では、重複したシグネチャに基づいた処理を行う結果、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができないという問題がある。以下に、図12および図13を用いて、この問題を具体的に説明する。図12および図13は、従

来技術に係るネットワーク攻撃防御システムを説明するための図である。

【 0 0 0 7 】

図 1 2 に示すように、中継装置 9-1 は、2 つの通信端末 3 0 がネットワーク上のサーバ 2 0 に対する D D o S 攻撃を行っていることを検出すると（同図の（1）参照）、シグネチャを隣接中継装置となる中継装置 9-2 および中継装置 9-3 に送信する（同図の（2）参照）。そして、隣接中継装置となる中継装置 9-1 からシグネチャを受信した中継装置 9-2 は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャを隣接中継装置となる中継装置 9-3 に送信する。同様に、隣接中継装置となる中継装置 9-1 からシグネチャを受信した中継装置 9-3 は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャを隣接中継装置となる中継装置 9-2 に送信する（同図の（3）参照）。なお、図 1 2 に示す例では、隣接中継装置からシグネチャを受信した中継装置 9 は、自己に送信した隣接中継装置にはシグネチャを送信しない。

【 0 0 0 8 】

このようなシグネチャの送信が行われると、図 1 2 に示す例では、中継装置 9-3 は、隣接中継装置となる中継装置 9-1 および中継装置 9-2 から同一のシグネチャを受信することになる。また、これと同様に、中継装置 9-2 も、隣接中継装置となる中継装置 9-1 および中継装置 9-3 から同一のシグネチャを受信することになる。その結果、中継装置 9-2 および中継装置 9-3 では、重複したシグネチャに基づいたパケット制御処理を行うことになり、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができない。

【 0 0 0 9 】

また、図 1 3 に示すように、中継装置 9-1 は、2 つの通信端末 3 0 がネットワーク上のサーバ 2 0 に対する D D o S 攻撃を行っていることを検出すると（同図の（1）参照）、シグネチャを隣接中継装置となる中継装置 9-2 および中継装置 9-3 に送信する（同図の（2）参照）。そして、隣接中継装置となる中継装置 9-1 からシグネチャを受信した中継装置 9-2 および中継装置 9-3 は、受信したシグネチャに基づいてパケットを処理するとともに、シグネチャをそれぞれの隣接中継装置となる中継装置 9-4 に送信する（同図の（3）参照）。

【 0 0 1 0 】

このようなシグネチャの送信が行われると、図 1 3 に示す例では、中継装置 9-4 は、隣接中継装置となる中継装置 9-2 および中継装置 9-3 から同一のシグネチャを受信することになる。その結果、中継装置 9-2 および中継装置 9-3 では、重複したシグネチャに基づいたパケット制御処理を行うことになり、シグネチャに基づいたパケットの規制に関する処理を効率的に行うことができない。

【 0 0 1 1 】

そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことが可能な中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

【課題を解決するための手段】

【 0 0 1 2 】

上述した課題を解決し、目的を達成するため、請求項 1 に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置であって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、を備えたことを特徴とする。

【0013】

また、請求項2に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

【0014】

また、請求項3に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手段を備え、当該シグネチャ生成手段は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。

【0015】

また、請求項4に係る発明は、上記の発明において、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を他の隣接中継装置に送信するとともに、当該シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、当該シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報および容疑シグネチャを前記シグネチャ記憶手段に対応付けて登録し、前記シグネチャ登録判定手段は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されている場合には、当該生成識別情報に対応付けて登録されている中継元情報が前記受信したシグネチャの中継元情報と同一であるか否かをさらに判定し、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記生成識別情報が前記シグネチャ記憶手段に既に登録されているが、前記中継元情報が同一であると判定された場合には、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に上書き登録するとともに、当該シグネチャを前記シグネチャ記憶手段に登録されている中継先情報が示す他の隣接中継装置に送信することを特徴とする。

【0016】

また、請求項5に係る発明は、上記の発明において、前記シグネチャ通信手段は、前記シグネチャ登録判定手段によって前記中継元情報が同一でないと判定された場合には、前記シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送し、さらに、当該既登録通知を他の隣接中継装置から受信した場合には、前記シグネチャ記憶手段に記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除することを特徴とする。

【0017】

また、請求項6に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、前記中継装置は、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手段と、前記識別情報判定手段によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手段と、を備えたことを特徴とする。

【0018】

また、請求項 7 に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継方法であって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定工程と、前記識別情報判定工程によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信工程と、を含んだことを特徴とする。

【 0 0 1 9 】

また、請求項 8 に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定工程は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信工程は、前記シグネチャ登録判定工程によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

【 0 0 2 0 】

また、請求項 9 に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成工程を含み、当該シグネチャ生成工程は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に対応付けて登録することを特徴とする。

【 0 0 2 1 】

また、請求項 10 に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャ記憶手段に登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、前記隣接中継装置から受信したシグネチャが前記シグネチャ記憶手段に既に登録されているか否かを判定するシグネチャ登録判定手順と、前記識別情報判定手順によって未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャを前記シグネチャ記憶手段に登録するとともに、当該シグネチャを他の隣接中継装置に送信するシグネチャ通信手順と、をコンピュータに実行させることを特徴とする。

【 0 0 2 2 】

また、請求項 11 に係る発明は、上記の発明において、前記シグネチャ記憶手段は、前記シグネチャの生成を一意に識別するための生成識別情報に対応付けて各シグネチャを記憶するものであって、前記シグネチャ登録判定手順は、前記隣接中継装置から受信したシグネチャの生成識別情報が前記シグネチャ記憶手段に既に登録されているか否かを判定し、前記シグネチャ通信手順は、前記シグネチャ登録判定手順によって前記生成識別情報が前記シグネチャ記憶手段に未だ登録されていないと判定された場合に、前記隣接中継装置から受信したシグネチャおよび生成識別情報を前記シグネチャ記憶手段に登録するとともに、当該シグネチャおよび生成識別情報を他の隣接中継装置に送信することを特徴とする。

【 0 0 2 3 】

また、請求項 12 に係る発明は、上記の発明において、攻撃容疑パケットの検出に応じてシグネチャを生成するとともに、当該シグネチャの生成識別情報を生成するシグネチャ生成手順をコンピュータに実行させ、当該シグネチャ生成手順は、前記シグネチャおよび生成識別情報を隣接中継装置に送信するとともに、当該中継先である隣接中継装置を特定するための中継先情報、前記生成識別情報およびシグネチャを前記シグネチャ記憶手段に

対応付けて登録することを特徴とする。

【発明の効果】

【0024】

請求項1、6、7または10の発明によれば、隣接中継装置から受信したシグネチャが既に登録されているか否かを判定して、未だ登録されていないシグネチャのみをシグネチャ記憶手段（シグネチャリスト）に登録するとともに隣接中継装置に送信するので、シグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

【0025】

また、請求項2、8または11の発明によれば、シグネチャの生成を一意に識別するための生成識別情報（生成元である中継装置を一意に識別するための識別子および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子からなる生成識別情報）を各シグネチャに対応付けて管理するので、シグネチャの具体的な内容にまで踏み込むことなく、生成識別情報のみからシグネチャが既に登録されているか否かを判定することが可能になる。また、シグネチャの内容が同一であっても生成識別情報（生成元）が異なっていれば、未だ登録されていないシグネチャであるとしてシグネチャリストに登録するとともに隣接中継装置に送信するので、生成元となる各中継装置の性能違い（例えば、攻撃検出や防御解除に係るアルゴリズムの違いなど）が尊重され、安全性の高いパケット制御を行うことが可能になる。

【0026】

また、請求項3、9または12の発明によれば、攻撃容疑パケットを検出すると、シグネチャおよび生成識別情報を生成し、これらシグネチャおよび生成識別情報を隣接中継装置に送信するとともに、中継先である隣接中継装置を特定するための中継先情報、生成識別情報およびシグネチャをシグネチャリストに対応付けて登録するので、シグネチャに対して確実に生成識別情報を付与することが可能になる。また、送信ミスや内容更新等に起因してシグネチャを再送信する必要性が生じた場合でも、シグネチャリストに登録された中継先情報、生成識別情報およびシグネチャを参照することで、同一の生成識別情報が付与されたシグネチャを同一の中継先に対して確実に再送信することが可能になる。

【0027】

また、請求項4の発明によれば、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに未だ登録されていない場合には、これを他の隣接中継装置に送信するとともに、シグネチャの直前の中継元である隣接中継装置を特定するための中継元情報、シグネチャの直後の中継先である隣接中継装置を特定するための中継先情報、生成識別情報およびシグネチャをシグネチャリストに対応付けて登録する。そして、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに既に登録されている場合には、中継元情報が同一であるか否かをさらに判定し、これが同一である場合には、シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている中継先情報が示す他の隣接中継装置にシグネチャを送信するので、送信ミスや内容更新等に起因してシグネチャが再送信されてきた場合でも、このシグネチャを留めることなく、中継先に対して確実に再送信することが可能になる。その一方、中継元情報が同一でない場合には、シグネチャの再送信でもないとは判定される結果、シグネチャの重複登録や重複送信を確実に回避することが可能になる。

【0028】

また、請求項5の発明によれば、隣接中継装置から受信したシグネチャの生成識別情報がシグネチャリストに既に登録されており、かつ、中継元情報も同一でない場合には、シグネチャの中継元である隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。さらに、当該既登録通知を他の隣接中継装置から受信した場合には、シグネチャリストに記憶された中継先情報から当該隣接中継装置に対応する中継先情報を削除する。したがって、送信ミスや内容更新等に起因してシグネチャを再送信する必要性が生じた場合でも、シグネチャリストから削除された中継先に対してはシグネチ

ャが送信されないことになり、シグネチャの再送信に際してもシグネチャの重複登録や重複送信を確実に回避することが可能になる。

【発明を実施するための最良の形態】

【0029】

以下に添付図面を参照して、この発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムの実施例を詳細に説明する。なお、以下では、本実施例で用いる主要な用語、ネットワーク攻撃防御システムの概要および特徴、中継装置の構成および処理、本実施例の効果を順に説明し、最後に本実施例に対する種々の変形例を説明する。

【実施例】

【0030】

〔用語の説明〕

まず最初に、本実施例で用いる主要な用語を説明する。本実施例で用いる「容疑シグネチャ」とは、攻撃容疑のあるパケット（攻撃容疑パケット）を制限するためのシグネチャであり、具体的には、通過が制限される攻撃容疑パケットの特徴を示す属性（例えば、宛先IPアドレス、プロトコル、宛先ポート番号など）や制限内容（例えば、特定のパケットが流入するときの帯域を制限するための制限情報など）を規定して構成される。

【0031】

また、本実施例で用いる「正規シグネチャ」とは、容疑シグネチャに該当するパケットのなかから攻撃とはみなされない正規パケット（正規ユーザの通信パケットである正規パケット）の通過を許可するためのシグネチャであり、具体的には、通過が許可される正規パケットの特徴を示す属性（例えば、送信元IPアドレス、サービスタイプ、宛先IPアドレス、プロトコル、宛先ポート番号など）を規定して構成される。

【0032】

また、本実施例で用いる「不正シグネチャ」とは、不正トラヒックに含まれる不正パケット（不正トラヒック条件を満たすパケット）を制限するためのシグネチャであり、具体的には、不正パケットの送信元IPアドレス等を規定して構成される。

【0033】

また、本実施例で用いる「識別情報（特許請求の範囲に記載の「生成識別情報」に対応する）」とは、上記したシグネチャの生成を一意に識別するための情報であり、具体的には、シグネチャの生成元である中継装置を一意に識別するための識別子（例えば、エンジンタイプ、エンジンIDおよびノードIDからなる識別子）および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子（例えば、シーケンシャルに付与される生成番号）から構成される。

【0034】

また、本実施例で用いる「下流ノード（特許請求の範囲に記載の「中継元情報」に対応する）」とは、上記したシグネチャを隣接する中継装置から受信して他の隣接する中継装置に送信した中継装置において、当該シグネチャの直前の中継元である隣接中継装置（すなわち、どの中継装置からシグネチャを受信したか）を特定するための情報であり、具体的には、隣接中継装置のアドレスを規定して構成される。

【0035】

また、本実施例で用いる「上流ノード（特許請求の範囲に記載の「中継先情報」に対応する）」とは、上記したシグネチャを隣接する中継装置から受信して他の隣接する中継装置に送信した中継装置において、当該シグネチャの直後の中継先である隣接中継装置（すなわち、どの中継装置に対してシグネチャを送信したか）を特定するための情報であり、具体的には、隣接中継装置のアドレスを規定して構成される。なお、シグネチャの中継元（下流ノード）は常に一つであるが、中継先（上流ノード）は複数になり得る。

【0036】

〔システムの概要および特徴〕

次に、図1を用いて、本実施例に係るネットワーク攻撃防御システムの概要および特徴

を説明する。図1は、本実施例に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

【0037】

同図に示すように、このネットワーク攻撃防御システム100は、ネットワーク上に複数の中継装置10を備えて構成される。また、このネットワーク上には、D o S攻撃やD D o S攻撃の対象となるコンピュータとしてのサーバ20や、かかるD o S攻撃やD D o S攻撃を行い得るコンピュータとしての通信端末30が接続されている。なお、以下では、図示した中継装置10の各々を区別する場合には、それぞれ中継装置10-1～中継装置10-7とし、サーバ20の各々を区別する場合には、サーバ20-1またはサーバ20-2とし、通信端末30の各々を区別する場合には、通信端末30-1～通信端末30-5として記載する。

【0038】

ここで、中継装置10の原則的な機能を最初に説明すると、中継装置10は、通信端末30のうち少なくとも1つ以上の通信端末30がネットワーク上のサーバ20に対してD o S攻撃またはD D o S攻撃を行っていることを検出した場合に、パケットの通過を制御するためのシグネチャ（容疑シグネチャや不正シグネチャ）を生成するとともに、パケットの通過を許可するための正規シグネチャを生成する。そして、中継装置10は、自ら生成したシグネチャ（容疑シグネチャ、不正シグネチャおよび正規シグネチャ）をシグネチャリストに登録する。

【0039】

また、中継装置10は、生成した容疑シグネチャ（さらには、正規シグネチャの生成に用いた正規条件）を隣接中継装置に送信する。さらに、中継装置10は、容疑シグネチャの生成直後だけでなく、送信ミスや内容更新等に起因して容疑シグネチャを再送信する必要がある場合にも、容疑シグネチャ等を改めて隣接中継装置に送信する。

【0040】

その一方で、中継装置10は、隣接中継装置から容疑シグネチャ等を受信した場合には、原則として、正規条件に基づいて正規シグネチャを生成するとともに、受信した容疑シグネチャおよび生成した正規シグネチャをシグネチャリストに登録し、さらに、受信した容疑シグネチャおよび正規条件を他の隣接中継装置に送信する。なお、隣接中継装置について例を挙げると、図1において、中継装置10-3における隣接中継装置は、中継装置10-1、中継装置10-2、中継装置10-4および中継装置10-7であり、中継装置10-5および中継装置10-6とは、隣接関係をもたない。また、この隣接関係は、物理的な隣接を意味するものではない。

【0041】

このようにして、図1に示したネットワーク攻撃防御システム100では、シグネチャを受信した各中継装置10がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置10が同様の容疑シグネチャや正規シグネチャをシグネチャリストに登録することになる。そして、各中継装置10では、かかるシグネチャリストに登録されたシグネチャに基づいてパケットの通過を制御する。つまり、不正シグネチャや容疑シグネチャに該当するパケットについては、伝送帯域を制限して通過させるかもしくは廃棄し、正規シグネチャに該当するパケットやいずれのシグネチャにも該当しないパケットについては、伝送帯域を制限せずに通過を許可する。

【0042】

ところで、本実施例における中継装置10は、上記したような原則的な機能に加えて、隣接中継装置から受信したシグネチャがシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合に限り、シグネチャをシグネチャリストに登録するとともに隣接中継装置に送信するようにしている点に主たる特徴がある。つまり、隣接中継装置から受信したシグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことができるようにしている。

【0043】

ここで、上記の主たる特徴を実現するために中継装置 10 が備える特徴的な機能を説明すると、容疑のかかる攻撃を検出した中継装置 10 では、攻撃容疑パケットを制限するための容疑シグネチャおよび容疑シグネチャの生成を一意に識別するための識別情報を生成する。そして、これら容疑シグネチャおよび識別情報を対応付けてシグネチャリストに登録するとともに、生成した容疑シグネチャ（さらには正規条件）および識別情報を隣接中継装置に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継先である隣接中継装置を特定するための上流ノードを容疑シグネチャおよび識別情報に対応付けてシグネチャリストに登録する。そして、容疑シグネチャを再送信する必要が生じた場合には、かかるシグネチャリストを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

【0044】

一方、容疑シグネチャおよび識別情報を受信した中継装置 10 では、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合には、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードを容疑シグネチャおよび識別情報に対応付けてシグネチャリストに登録する。

【0045】

また、容疑シグネチャ等を受信した中継装置 10 では、上記とは反対に、受信した容疑シグネチャの識別情報がシグネチャリストに既に登録されている場合には、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かをさらに判定する。そして、下流ノードが同一である場合には、シグネチャの再送信であるとして、受信した容疑シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている上流ノードが示す他の隣接中継装置にシグネチャを再送信する。

【0046】

その一方、容疑シグネチャ等を受信した中継装置 10 では、上記した判定において下流ノードが同一でない場合には、シグネチャの再送信でもないとして、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）すること、他の隣接中継装置に送信（または再送信）すること、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を隣接中継装置から受信した中継装置 10 では、シグネチャリストに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。

【0047】

以下に、図 1 を用いて、上記した主たる特徴が実現される具体例を説明する。同図に示すように、例えば、通信端末 30-4 および通信端末 30-5 がサーバ 20-1 に対する D o S 攻撃を行っており、中継装置 10-1 が容疑のかかる攻撃を検出したとすると、中継装置 10-1 は、攻撃容疑パケットを制限するための容疑シグネチャおよび識別情報を生成し、これら容疑シグネチャおよび識別情報を対応付けてシグネチャリストに登録するとともに、生成した容疑シグネチャ（さらには正規条件）および識別情報を隣接中継装置である中継装置 10-2 および中継装置 10-3 に送信する。さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継装置 10-2 および中継装置 10-3 のアドレスを上流ノードとしてシグネチャリストに登録する（図 1 の（1）および（2）参照）。

【0048】

一方、中継装置 10-2 および中継装置 10-3 は、中継装置 10-1 から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定するが、ここでは、識別情報が未だ登録されていないので、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。つまり、中継装

置 10-2 は、中継装置 10-4 に容疑シグネチャおよび識別情報を送信し、また、中継装置 10-3 は、中継装置 10-4 および中継装置 10-7 に容疑シグネチャおよび識別情報を送信する（同図の（3）および（4）参照）。

【0049】

さらに、かかる容疑シグネチャおよび識別情報の中継に応じて、中継装置 10-2 および中継装置 10-3 は、下流ノードおよび上流ノードの情報をシグネチャリストに登録する。つまり、中継装置 10-2 は、中継装置 10-1 のアドレスを下流ノードとして、中継装置 10-4 のアドレスを上流ノードとしてシグネチャリストに登録し、また、中継装置 10-3 は、中継装置 10-1 のアドレスを下流ノードとして、中継装置 10-4 および中継装置 10-7 のアドレスを上流ノードとしてシグネチャリストに登録する。

【0050】

そして、中継装置 10-7 は、中継装置 10-3 から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報は自己のシグネチャリストに未だ登録されていないので、上記した中継装置 10-2 および中継装置 10-3 と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するが、隣接中継装置がないので、当該容疑シグネチャおよび識別情報を隣接中継装置に送信することはしない。さらに、中継装置 10-7 は、上流ノードは登録しないが、中継装置 10-3 のアドレスを下流ノードとしてシグネチャリストに登録する（同図の（5）参照）。

【0051】

その一方、中継装置 10-4 は、例えば、中継装置 10-2 から中継装置 10-3 よりも先に容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに未だ登録されていないので、上記した中継装置 10-2 および中継装置 10-3 と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置となる中継装置 10-3、中継装置 10-5 および中継装置 10-6 に送信する。さらに、中継装置 10-4 は、中継装置 10-2 のアドレスを下流ノードとしてシグネチャリストに登録するとともに、中継装置 10-3、中継装置 10-5 および中継装置 10-6 のアドレスを上流ノードとしてシグネチャリストに登録する（図（6）および（7）参照）。

【0052】

そして、中継装置 10-5 および中継装置 10-6 は、中継装置 10-4 から容疑シグネチャおよび識別情報を受信すると、受信した容疑シグネチャの識別情報が自己のシグネチャリストに未だ登録されていないので、上記した中継装置 10-7 と同様、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するが、隣接中継装置がないので、当該容疑シグネチャおよび識別情報を隣接中継装置に送信することはしない。さらに、中継装置 10-5 および中継装置 10-6 は、上流ノードは登録しないが、中継装置 10-4 のアドレスを下流ノードとしてシグネチャリストに登録する（同図の（8）参照）。

【0053】

ところで、中継装置 10-4 は、上記した例によって、中継装置 10-2 から容疑シグネチャおよび識別情報を受信した後、中継装置 10-3 から同一の容疑シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されており、かつ、識別情報に対応付けて登録されている下流ノード（中継装置 10-2）が現に受信したシグネチャの下流ノード（中継装置 10-3）と同一でないので、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）すること、他の隣接中継装置に送信（または再送信）すること、受信したシグネチャの下流ノードである中継装置 10-2 に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を中継装置 10-4 から受信した中継装置 10-3 では、シグネチャリストに記憶された当該シグネチャの上流ノードから中継装置 10-4 のアドレスを削除する。

【0054】

また、中継装置 10-3 は、上記した例によって、中継装置 10-4 から同一の容疑

シグネチャおよび識別情報を受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されており、かつ、識別情報に対応付けて登録されている下流ノード（中継装置１０－１）が現に受信したシグネチャの下流ノード（中継装置１０－４）と同一でないので、受信した容疑シグネチャをシグネチャリストに登録（または上書き登録）すること、他の隣接中継装置に送信（または再送信）すること、受信したシグネチャの下流ノードである中継装置１０－４に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。そして、かかる既登録通知を中継装置１０－３から受信した中継装置１０－４では、シグネチャリストに記憶された当該シグネチャの上流ノード（中継装置１０－３、中継装置１０－５および中継装置１０－６のアドレス）から中継装置１０－３のアドレスを削除する。

【００５５】

さらに、中継装置１０－４は、上記した例によって、中継装置１０－２から容疑シグネチャおよび識別情報を受信した後、同じく中継装置１０－２から同一の識別情報からなる容疑シグネチャを受信した場合には、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているが、識別情報に対応付けて登録されている下流ノード（中継装置１０－２）が現に受信したシグネチャの下流ノード（中継装置１０－２）と同一であるので、シグネチャの再送信であるとして、受信した容疑シグネチャをシグネチャリストに上書き登録するとともに、シグネチャリストに登録されている上流ノード（中継装置１０－５および中継装置１０－６のアドレス）が示す中継装置１０－５および中継装置１０－６に容疑シグネチャを再送信する。

【００５６】

以上のように、図１に示したネットワーク攻撃防御システムでは、隣接中継装置から受信したシグネチャがシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合に限り、シグネチャをシグネチャリストに登録するとともに隣接中継装置に送信するようにすることで、上記した例で言えば、中継装置１０－４や中継装置１０－３においてシグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

【００５７】

なお、中継装置１０は、攻撃を防御しながらパケットを中継するための装置であり、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、中継装置１０は、中継装置１０等を管理するための管理用ネットワークに接続されていてもよく、シグネチャは、管理用ネットワークを介して送受されてもよい。さらに、中継装置１０が送信するシグネチャは、容疑シグネチャだけに限定されず、中継装置１０は、他のシグネチャを送信してもよく、容疑シグネチャに加えて他のシグネチャを送信するようにしてもよい。

【００５８】

〔中継装置の構成〕

次に、図２を用いて、図１に示した中継装置１０の構成を説明する。図２は、中継装置１０の構成を示すブロック図である。同図に示すように、この中継装置１０は、ネットワークインタフェース１１と、パケット取得部１２と、攻撃検出部１３（並びに攻撃容疑検出条件テーブル１３ａ、不正トラヒック検出条件テーブル１３ｂおよび正規条件テーブル１３ｃ）と、シグネチャ通信部１４と、識別情報判定部１５と、フィルタ部１６（並びにシグネチャリスト１６ａ）とを備えて構成される。

【００５９】

また、中継装置１０は、ＣＰＵ（Central Processing Unit）やメモリ、ハードディスク等を有しており、パケット取得部１２、攻撃検出部１３、シグネチャ通信部１４、識別情報判定部１５およびフィルタ部１６は、ＣＰＵによって処理されるプログラムのモジュールであってもよい。また、このプログラムのモジュールは、１つのＣＰＵで処理されてもよく、複数のＣＰＵに分散して処理されてもよい。さらに、中継装置１０には、Linux等の汎用ＯＳをインストールしておき、汎用ＯＳに具備されるパケットフィルタをフ

イルタ部 16 として機能させてもよい。

【0060】

なお、攻撃検出部 13 は特許請求の範囲に記載の「シグネチャ生成手段」に対応し、シグネチャ通信部 14 は同じく「シグネチャ通信手段」に対応し、識別情報判定部 15 は同じく「シグネチャ登録判定手段」に対応し、シグネチャリスト 16 a は同じく「シグネチャ記憶手段」に対応する。

【0061】

図 2 において、ネットワークインタフェース部 11 は、ネットワークと接続されている通信機器との間でパケットを送受する手段であり、具体的には、LAN (Local Area Network) または WAN (Wide Area Network) などのネットワークと接続するためのネットワーク接続カード等によって構成される。なお、図 2 には示していないが、キーボードやマウス、マイクなど、ネットワーク管理者から各種の情報や指示の入力を受付ける入力手段や、モニタ（若しくはディスプレイ、タッチパネル）やスピーカなど、各種の情報を出力する出力手段を備えて中継装置 10 を構成するようにしてもよい。

【0062】

パケット取得部 12 は、ネットワークインタフェース部 11 が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部 13 およびパケット数判定部 15 a に提供する処理部である。

【0063】

攻撃検出部 13 は、パケット取得部 12 によって提供された統計情報に基づいて、攻撃の検出および攻撃の分析を行う処理部であり、図 2 に図示するように、攻撃容疑検出条件テーブル 13 a、不正トラヒック検出条件テーブル 13 b および正規条件テーブル 13 c にそれぞれ接続される。ここで、各テーブル 13 a ~ 13 c に記憶される情報を具体的に説明した後に、攻撃検出部 13 による処理内容を説明する。

【0064】

図 3 は、攻撃容疑検出条件テーブル 13 a に記憶される情報、より詳細には、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用される「攻撃容疑検出条件」の一例を示す図である。同図に示すように、攻撃容疑検出条件は、検出属性、検出閾値および検出間隔の組合せからなる複数組（ここでは 3 組）のレコードで構成され、かかる攻撃容疑検出条件の各レコードの内のいずれかのレコードの条件にトラヒックが一致した場合に、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。なお、番号はレコードを特定するために便宜上使用されるものである。

【0065】

攻撃容疑検出条件の「検出属性」には、例えば、IP パケットに含まれる IP ヘッダ部の属性や、IP パケットのペイロード部に含まれる TCP ヘッダ部または UDP ヘッダ部の属性が指定される。具体的には、図 3 において、番号 1 のレコードの検出属性は、「Destination IP Address (宛先 IP アドレス)」が「192.168.1.1/32」であり (dst=192.168.1.1/32)、IP の上位層 (TCP または UDP) のプロトコル種別を示す「Protocol (プロトコル)」が「TCP」であり (Protocol=TCP)、かつ、IP の上位層プロトコルがどのアプリケーションの情報であることを示す「Destination Port (宛先ポート番号)」が「80」である (Port=80) という属性値の組で指定される。

【0066】

また、番号 2 のレコード検出属性は、「Destination IP Address (宛先 IP アドレス)」が「192.168.1.2/32」であり (dst=192.168.1.2/32)、かつ、「Protocol (プロトコル)」が「UDP (User Datagram protocol)」である (Protocol=UDP) という属性値の組で指定される。同様に、番号 3 のレコード検出属性は、「Destination IP Address (宛先 IP アドレス)」が「192.168.1.0/24」という属性で指定される。

【0067】

攻撃容疑検出条件の「検出閾値」は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を指定し

たものであり、攻撃容疑検出条件の「検出間隔」は、同じく最低の連続時間を指定したものである。なお、図3には示していないが、検出属性においては、「Destination IP Address（宛先IPアドレス）」の値を無条件（any）とし、かつ、IPの上位層のプロトコル種別を示す「Protocol（プロトコル）」が「ICMP（Internet Control Message Protocol）」となる属性値の組を指定するようにしてもよい。

【0068】

図4は、不正トラヒック検出条件テーブル13bに記憶される情報、より詳細には、攻撃容疑パケットのトラヒックから不正トラヒックを検出するために用いられる「不正トラヒック条件」の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のDDoS攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。なお、番号はレコード（パターン）を特定するために便宜上使用されるものである。

【0069】

具体的には、番号1の不正トラヒック条件は、「伝送帯域T1Kbps以上、パケットがS1秒以上連続送信されている」というトラヒックパターンを示している。また、番号2の不正トラヒック条件は、「伝送帯域T2Kbps以上、ICMP（Internet Control Message Protocol）上のエコー応答（Echo Reply）メッセージのパケットがS2秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号3の不正トラヒック条件は、「伝送帯域T3Kbps以上、データが長すぎるためパケットに含まれるデータは複数IPパケットに分割して送信していることを示すフラグメントパケットがS3秒以上連続送信されている」というトラヒックパターンを示している。

【0070】

図5は、正規条件テーブル13cに記憶される情報、より詳細には、正当な利用者が利用している通信端末30から送信されるパケットを表す「正規条件」の一例を示す図である。同図に示すように、正規条件は、IPパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード（パターン）を特定するために便宜上使用されるものである。

【0071】

具体的には、番号1のレコードの検出属性は、IPの「Source IP Address（送信元IPアドレス）」が「172.16.10.0/24」であることを指定し（src=172.16.10.0/24）、番号2のレコードの検出属性はIP上のサービス品質を示す「Type of Service（サービスタイプ）」が「（16進で）01」であることを指定している（TOS=0x01）。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ20等の送信元IPアドレスが設定され、サーバ20が収容されているLANの所有者が正規ユーザであると認識しているネットワークの送信元IPアドレスなどが設定される。

【0072】

図2の説明に戻ると、攻撃検出部13は、パケット取得部12によって提供された統計情報に基づいて攻撃の検出を検出した場合に、攻撃容疑トラヒックの通信パケット（攻撃容疑パケット）を制限するための容疑シグネチャを生成する。具体的には、攻撃検出部13は、図3に示した攻撃容疑検出条件に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、各レコードの内のいずれかのレコードに合致した場合には、このトラヒックを攻撃容疑トラヒックとして検出し、このときに検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を容疑シグネチャとして生成する。

【0073】

また、攻撃検出部13は、攻撃を検出した場合に、容疑シグネチャとともに正規シグネチャを生成する。具体的には、図5に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのAND条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケッ

トを許可するために用いられるシグネチャであるが、例えば、図3および図5の例を用いて説明すると、図3における番号1のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32, Protocol=TCP, Port=80]となり、図5において、正規シグネチャは、[src=172.16.10.24, dst=192.168.1.1/32, Protocol=TCP, Port=80]および[TOS=0x01, dst=192.168.1.1/32, Protocol=TCP, Port=80]となる。

【0074】

さらに、攻撃検出部13は、図4に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元IPアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

【0075】

上述してきた攻撃検出部13によって生成された容疑シグネチャ、正規シグネチャおよび不正シグネチャは、シグネチャリスト16a（図6参照）に登録される。そして、攻撃検出部13は、各シグネチャの生成を一意に識別するための識別情報を生成し、この識別情報とともにシグネチャをシグネチャリスト16aに登録する。

【0076】

ここで、図7を参照して、シグネチャに付与される識別情報を説明する。図7は、シグネチャに付与される識別情報の例を示す図であるが、同図に示すように、攻撃検出部13は、シグネチャの生成元である中継装置10を一意に識別するための識別子（すなわち、エンジンタイプ、エンジンIDおよびノードIDからなる識別子）および当該中継装置で生成される複数の容疑シグネチャをそれぞれ一意に識別するための識別子（例えば、シーケンシャルに付与される生成番号）から構成される識別情報を生成する。

【0077】

図2において、シグネチャ通信部14は、攻撃検出部13が生成したシグネチャ等を隣接中継装置に送信するとともに、隣接中継装置から送信されたシグネチャを受信し、また、隣接中継装置から受信したシグネチャをシグネチャリスト16aに登録し、さらに、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理部である。

【0078】

具体的には、シグネチャ通信部14は、攻撃検出部13によってシグネチャおよび識別情報がシグネチャリスト16aに登録されると、登録されたシグネチャ等を識別情報とともに隣接中継装置に送信する。さらに、シグネチャ通信部14は、かかるシグネチャおよび識別情報の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト16aに登録する（図6参照）。そして、シグネチャ通信部14は、容疑シグネチャ等を再送信する必要がある場合には、かかるシグネチャリスト16aを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

【0079】

また、シグネチャ通信部14は、隣接中継装置から受信したシグネチャをシグネチャリスト16aに登録する処理および他の隣接中継装置に送信する処理を行うが、かかる処理は、以下に説明する識別情報判定部15による判定結果に従って実行される。

【0080】

識別情報判定部15は、シグネチャ通信部14によって隣接中継装置からシグネチャを受信した場合に、受信したシグネチャの識別情報がシグネチャリスト16aに既に登録されているか否かを判定する。そして、未だ登録されていないと識別情報判定部15が判定した場合には、上記のシグネチャ通信部14は、受信したシグネチャおよび識別情報をシグネチャリスト16aに登録するとともに、当該シグネチャおよび識別情報を隣接中継装置に送信する。さらに、シグネチャ通信部14は、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト16aに登録する（図6参照）。

【0081】

これとは反対に、受信したシグネチャの識別情報がシグネチャリスト16aに既に登録されている場合には、識別情報判定部15は、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かをさらに判定する。そして、下流ノードが同一であると識別情報判定部15が判定した場合には、上記のシグネチャ通信部14は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト16aに上書き登録するとともに、シグネチャリスト16aに登録されている上流ノードが示す他の隣接中継装置にシグネチャを再送信する。

【0082】

さらに、上記した判定において、下流ノードが同一でないと識別情報判定部15が判定した場合には、上記のシグネチャ通信部14は、シグネチャの再送信でもないとして、受信した容疑シグネチャをシグネチャリスト16aに登録（または上書き登録）すること、他の隣接中継装置に送信（または再送信）すること、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。その一方、シグネチャ通信部14は、かかる既登録通知を隣接中継装置から受信した場合には、シグネチャリスト16aに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。

【0083】

図2において、フィルタ部16は、ネットワークインタフェース部11が受信したパケットを受け入れて、シグネチャリスト16aに基づいてパケットの通過（ネットワークインタフェース部11からのパケットの出力）を制御する処理部である。具体的には、入力されたパケットについて、シグネチャリスト16aに登録された「不正シグネチャ」、「正規シグネチャ」、「容疑シグネチャ」のいずれかに該当するか（もしくはいずれにも該当しないか）を判別した上で、該当するシグネチャに基づいてパケットの通過を制御する。

【0084】

より詳細には、フィルタ部16は、不正シグネチャに該当するパケットは、不正なパケットを処理するための不正キューに入力し、容疑シグネチャに該当するパケットは、容疑ユーザ用の容疑キューに入力し、正規シグネチャに該当するパケットまたはいずれのシグネチャにも該当しないパケットは、正規ユーザ用の正規キューに入力する。その上で、フィルタ部16は、正規キューに入力されたパケットについては、伝送帯域を制限せずにネットワークインタフェース部11から出力し、容疑キューおよび不正キューに入力されたパケットについては、それぞれのシグネチャ（条件を満たすとして選択されたシグネチャ）が示す伝送帯域制限値に従って制限して出力する。

【0085】

なお、フィルタ部16は、シグネチャリスト16aに登録されたシグネチャの検出属性等が所定の解除判断基準を満たした場合には、この所定の解除判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいてパケットの通過を制御する処理を停止する。

【0086】

【攻撃容疑パケット検出時の処理】

続いて、図8を参照して、上記した中継装置10による攻撃容疑パケット検出時の動作処理を説明する。図8は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。

【0087】

同図に示すように、中継装置10の攻撃検出部13は、図3に示した攻撃容疑検出条件テーブル13aに基づいて攻撃容疑トラヒックを検出すると（ステップS1）、容疑シグネチャおよび正規シグネチャを生成する（ステップS2）。

【0088】

そして、攻撃検出部13は、各シグネチャの生成を一意に識別するための識別情報を生

成し（ステップS 3）、この識別情報とともに容疑シグネチャおよび正規シグネチャをフィルタ部16のシグネチャリスト16aに登録する（ステップS 4）。さらに、シグネチャ通信部14は、攻撃検出部13が生成したシグネチャ等（本実施例では、容疑シグネチャおよび正規条件）を識別情報とともに隣接中継装置に送信する（ステップS 5）。

【0089】

なお、シグネチャ通信部14は、上記したステップS 4によるシグネチャ等の中継に応じて、中継先である隣接中継装置を特定するための上流ノードをシグネチャリスト16aに登録する。そして、シグネチャ通信部14は、容疑シグネチャ等を再送信する必要が生じた場合には、かかるシグネチャリスト16aを参照して、同一の識別情報が付与されたシグネチャを同一の中継先である隣接中継装置に対して再送信する。

【0090】

〔シグネチャ受信時の処理〕

続いて、図9を参照して、上記した中継装置10によるシグネチャ受信時の動作処理を説明する。図9は、シグネチャ受信時の処理手順を示すフローチャートである。

【0091】

同図に示すように、中継装置10のシグネチャ通信部14が、隣接中継装置から送信されたシグネチャ等（本実施例では、容疑シグネチャおよび正規条件）を受信すると（ステップS 11）、識別情報判定部15は、受信したシグネチャの識別情報がフィルタ部16のシグネチャリスト16aに既に登録されているか否かを判定し（ステップS 12）、さらに、かかる識別情報がシグネチャリスト16aに既に登録されている場合には（ステップS 12肯定）、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であるか否かも判定する（ステップS 13）。

【0092】

かかる判定において、識別情報がシグネチャリスト16aに既に登録されているおり、かつ、下流ノードが同一でないと識別情報判定部15が判定した場合には（ステップS 12肯定かつステップS 13否定）、シグネチャ通信部14は、受信した容疑シグネチャをシグネチャリスト16aに登録（または上書き登録）すること、他の隣接中継装置に送信（または再送信）すること、受信したシグネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する（ステップS 131）。なお、かかる既登録通知を隣接中継装置から受信した中継装置10では、シグネチャリスト16aに記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。

【0093】

これとは反対に、受信したシグネチャの識別情報がシグネチャリスト16aに未だ登録されていないと識別情報判定部15が判定した場合には（ステップS 12否定）、シグネチャ通信部14は、受信したシグネチャおよび識別情報をフィルタ部16のシグネチャリスト16aに登録し（ステップS 14）、攻撃検出部13は、シグネチャ通信部14が受信した正規条件に基づいて正規シグネチャを生成するとともに（ステップS 15）、正規シグネチャをシグネチャリスト16aに登録する（ステップS 16）。

【0094】

さらに、シグネチャ通信部14は、シグネチャリスト16aに登録した容疑シグネチャおよび識別情報（さらには、正規シグネチャの生成に用いた正規条件）を隣接中継装置に送信する（ステップS 17）。なお、シグネチャ通信部14は、このステップS 17によるシグネチャ等の中継に応じて、中継元である隣接中継装置を特定するための下流ノードおよび中継先である隣接中継装置を特定するための上流ノードをシグネチャおよび識別情報に対応付けてシグネチャリスト16aに登録する。

【0095】

ところで、上記したステップS 13の判定において、受信したシグネチャの識別情報がシグネチャリスト16aに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一であると識別情報判定部15が

判定した場合には（ステップS 1 3 肯定）、シグネチャ通信部1 4は、シグネチャの再送信であるとして、受信したシグネチャをシグネチャリスト1 6 aに上書き登録するとともに（ステップS 1 3 2）、攻撃検出部1 3は、シグネチャ通信部1 4が受信した正規条件に基づいて正規シグネチャを再生成するとともに（ステップS 1 3 3）、正規シグネチャをシグネチャリスト1 6 aに上書き登録する（ステップS 1 3 4）。さらに、シグネチャ通信部1 4は、シグネチャリスト1 6 aに登録されている上流ノードが示す他の隣接中継装置に、容疑シグネチャおよび識別情報（さらには、正規シグネチャの生成に用いた正規条件）を再送信する（ステップS 1 3 5）。

【0 0 9 6】

なお、上記では、シグネチャの再送信であると判定された場合（受信したシグネチャの識別情報がシグネチャリスト1 6 aに既に登録されているが、識別情報に対応付けて登録されている下流ノードが現に受信したシグネチャの下流ノードと同一である場合）に、容疑シグネチャの上書き登録、正規シグネチャの再生成および上書き登録（ステップS 1 3 2～S 1 3 4）を行う場合を説明したが、本発明は必ずしもこれに限定されるものではなく、これらの処理（ステップS 1 3 2～S 1 3 4）を省いて、容疑シグネチャ、識別情報および正規条件の再送信（ステップS 1 3 5）のみを行うようにしてもよい。

【0 0 9 7】

〔不正パケット検出時の処理〕

続いて、図1 0を参照して、上記した中継装置1 0による不正パケット検出時の動作処理を説明する。図1 0は、不正パケット検出時の処理手順を示すフローチャートである。

【0 0 9 8】

同図に示すように、中継装置1 0の攻撃検出部1 7が、図4に示した不正トラヒック条件に基づいて不正トラヒックを検出すると（ステップS 2 1）、不正シグネチャを生成する（ステップS 2 2）。そして、攻撃検出部1 7は、生成した不正シグネチャをフィルタ部1 6のシグネチャリスト1 6 aに登録する（ステップS 2 3）。

【0 0 9 9】

〔パケット制御時の処理〕

続いて、図1 1を参照して、上記した中継装置1 0によるパケット制御時の動作処理を説明する。図1 1は、パケット制御時の処理手順を示すフローチャートである。

【0 1 0 0】

同図に示すように、フィルタ部1 6は、ネットワークインタフェース部1 1からパケットが入力されると（ステップS 3 1 肯定）、シグネチャリスト1 6 aに登録された不正シグネチャに合致するか否かを判断する（ステップS 3 2）。そして、不正シグネチャに合致した場合には（ステップS 3 2 肯定）、フィルタ部1 6は、不正なパケットを処理するための不正キューにパケットを入力する（ステップS 3 3）。

【0 1 0 1】

これとは反対に、不正シグネチャに合致しない場合には（ステップS 3 2 否定）、フィルタ部1 6は、入力されたパケットが、シグネチャリスト1 6 aに登録された正規シグネチャに合致するか否かを判断する（ステップS 3 4）。そして、正規シグネチャに合致した場合には（ステップS 3 4 肯定）、フィルタ部1 6は、正規なユーザ用の正規キューにパケットを入力する（ステップS 3 5）。

【0 1 0 2】

さらに、この正規シグネチャにも合致しない場合には（ステップS 3 4 否定）、フィルタ部1 6は、入力されたパケットが、シグネチャリスト1 6 aに登録された容疑シグネチャに合致するか否かを判断する（ステップS 3 6）。そして、容疑シグネチャに合致した場合には（ステップS 3 6 肯定）、フィルタ部1 6は、容疑ユーザ用の容疑キューにパケットを入力する（ステップS 3 7）。これとは反対に、容疑シグネチャに合致しない場合には（ステップS 3 6 否定）、フィルタ部1 6は、正規キューにパケットを入力する（ステップS 3 8）。

【0 1 0 3】

そして、フィルタ部 16 は、それぞれのキューにあるパケットについて、正規キューであれば、伝送帯域を制限せずにネットワークインタフェース部 11 から出力し、容疑キューおよび不正キューであれば、それぞれのシグネチャが示す伝送帯域制限値に従って制限して出力する。なお、不正シグネチャ、正規シグネチャ、容疑シグネチャの各シグネチャは、それぞれシグネチャリスト 16 a に複数登録されてもよい。また、登録されたシグネチャの検出属性等が所定の判断基準を満たした場合に、フィルタ部 16 は、所定の判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいたパケットの通過を制御する処理を停止する。

【0104】

【実施例の効果】

上述してきたように、上記の実施例によれば、隣接中継装置から受信したシグネチャが既に登録されているか否かを判定して、未だ登録されていないシグネチャのみをシグネチャリスト 16 a に登録するとともに隣接中継装置に送信するので、シグネチャの重複登録や重複送信が回避され、シグネチャに基づいたパケット制御を効率的に行うことが可能になる。

【0105】

また、上記の実施例によれば、シグネチャの生成を一意に識別するための識別情報を各シグネチャに対応付けて管理するので、シグネチャの具体的な内容にまで踏み込むことなく、識別情報のみからシグネチャが既に登録されているか否かを判定することが可能になる。さらに、シグネチャの内容が同一であっても識別情報（生成元）が異なっていれば、未だ登録されていないシグネチャであるとしてシグネチャリスト 16 a に登録するとともに隣接中継装置に送信するので、生成元となる各中継装置の性能違い（例えば、攻撃検出や防御解除に係るアルゴリズムの違いなど）が尊重され、安全性の高いパケット制御を行うことが可能になる。

【0106】

また、上記の実施例によれば、攻撃容疑パケットを検出すると、容疑シグネチャおよび識別情報を生成し、これらシグネチャおよび識別情報を隣接中継装置に送信するとともに、中継先である隣接中継装置を特定するための上流ノード、識別情報および容疑シグネチャをシグネチャリスト 16 a に対応付けて登録するので、シグネチャに対して確実に識別情報を付与することが可能になる。さらに、送信ミスや内容更新等に起因してシグネチャを再送信する必要がある場合でも、シグネチャリスト 16 a に登録された上流ノード、識別情報およびシグネチャを参照することで、同一の識別情報が付与されたシグネチャを同一の中継先に対して確実に再送信することが可能になる。

【0107】

また、上記の実施例によれば、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト 16 a に未だ登録されていない場合には、これを他の隣接中継装置に送信するとともに、シグネチャの直前の中継元である隣接中継装置を特定するための下流ノード、シグネチャの直後の中継先である隣接中継装置を特定するための上流ノード、識別情報およびシグネチャをシグネチャリスト 16 a に対応付けて登録する（図 6 参照）。そして、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト 16 a に既に登録されている場合には、下流ノードが同一であるか否かをさらに判定し、これが同一である場合には、シグネチャをシグネチャリスト 16 a に上書き登録するとともに、シグネチャリスト 16 a に登録されている上流ノードが示す他の隣接中継装置にシグネチャを送信するので、送信ミスや内容更新等に起因してシグネチャが再送信されてきた場合でも、このシグネチャを留めることなく、中継先に対して確実に再送信することが可能になる。その一方、下流ノードが同一でない場合には、シグネチャの再送信でもないと判定される結果、シグネチャの重複登録や重複送信を確実に回避することが可能になる。

【0108】

また、上記の実施例によれば、隣接中継装置から受信したシグネチャの識別情報がシグネチャリスト 16 a に既に登録されており、かつ、下流ノードも同一でない場合には、シ

グネチャの下流ノードである隣接中継装置に対して、当該シグネチャが既に登録されている旨を示す既登録通知を返送する。さらに、当該既登録通知を他の隣接中継装置から受信した場合には、シグネチャリスト 16 a に記憶された上流ノードから当該隣接中継装置に対応する情報（アドレス）を削除する。したがって、送信ミスや内容更新等に起因してシグネチャを再送信する必要が生じた場合でも、シグネチャリスト 16 a から削除された中継先に対してはシグネチャが送信されないことになり、シグネチャの再送信に際してもシグネチャの重複登録や重複送信を確実に回避することが可能になる。

【0109】

〔他の実施例〕

さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。

【0110】

例えば、上記の実施例では、シグネチャの生成を一意に識別するための生成識別情報に基づいて重複登録を判定する場合を説明したが、本発明はこれに限定されるものではなく、生成元となる各中継装置の性能を無視し、シグネチャの内容が同一であるか否かによって重複登録を判定するようにしてもよい。さらには、生成元となる各中継装置の性能を考慮し、シグネチャの内容が同一であり、かつ、生成元の性能が同一であるか否かによって重複登録を判定するようにしてもよい。

【0111】

また、各中継装置 10 は、受信した容疑シグネチャおよび識別情報を隣接中継装置に送信する前に、容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したか否かを判定するようにしてもよい。すなわち、所定の閾値を超過したと判定した場合に初めて（攻撃有りと判定した場合に初めて）、受信した容疑シグネチャを隣接中継装置に送信するようにしてもよい。例えば、図 1 に示した例で言えば、中継装置 10-4 は、通信端末 30-1～通信端末 30-3 によって攻撃がなされていないので、中継装置 10-2 または中継装置 10-3 から容疑シグネチャおよび識別情報を受信したとしても、所定の閾値を超過したと判定することはなく、容疑シグネチャを隣接中継装置となる中継装置 10-5 や中継装置 10-6 に送信しない。

【0112】

また、上記の実施例で図示した各装置（例えば、図 1 に例示した中継装置 10）の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、中継装置 10 の分散・統合の具体的形態は図示のものに限られず、中継装置 10 の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、中継装置 10 にて行なわれる各処理機能は、その全部または任意の一部が、CPU および当該 CPU にて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

【0113】

また、上記の実施例で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報（例えば、攻撃容疑検出条件テーブル、不正トラヒック検出条件テーブル、正規条件テーブルの内容等）については、特記する場合を除いて任意に変更することができる。

【0114】

なお、上記の実施例では、本発明を実現する各装置（例えば、中継装置 10）を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。すなわち、本実施例で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ

上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク（F D）、C D－R O M、M O、D V Dなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例に示したような中継装置用プログラムを格納したC D－R O Mを配布し、このC D－R O Mに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

【産業上の利用可能性】

【 0 1 1 5 】

以上のように、本発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムは、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャをシグネチャリストに登録してパケットの通過を制御するとともに、当該シグネチャを他の隣接中継装置に送信する場合に有用であり、特に、シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことに適する。

【図面の簡単な説明】

【 0 1 1 6 】

【図 1】 ネットワーク攻撃防御システムの構成を示すシステム構成図である。

【図 2】 中継装置の構成を示すブロック図である。

【図 3】 攻撃容疑検出条件テーブルに記憶される情報の例を示す図である。

【図 4】 不正トラヒック検出条件テーブルに記憶される情報の例を示す図である。

【図 5】 正規条件テーブルに記憶される情報の例を示す図である。

【図 6】 シグネチャリストに記憶される情報の例を示す図である。

【図 7】 シグネチャに付与される識別情報の例を示す図である。

【図 8】 攻撃容疑パケット検出時の処理手順を示すフローチャートである。

【図 9】 シグネチャ受信時の処理手順を示すフローチャートである。

【図 1 0】 不正パケット検出時の処理手順を示すフローチャートである。

【図 1 1】 パケット制御時の処理手順を示すフローチャートである。

【図 1 2】 従来技術に係るネットワーク攻撃防御システムを説明するための図である。

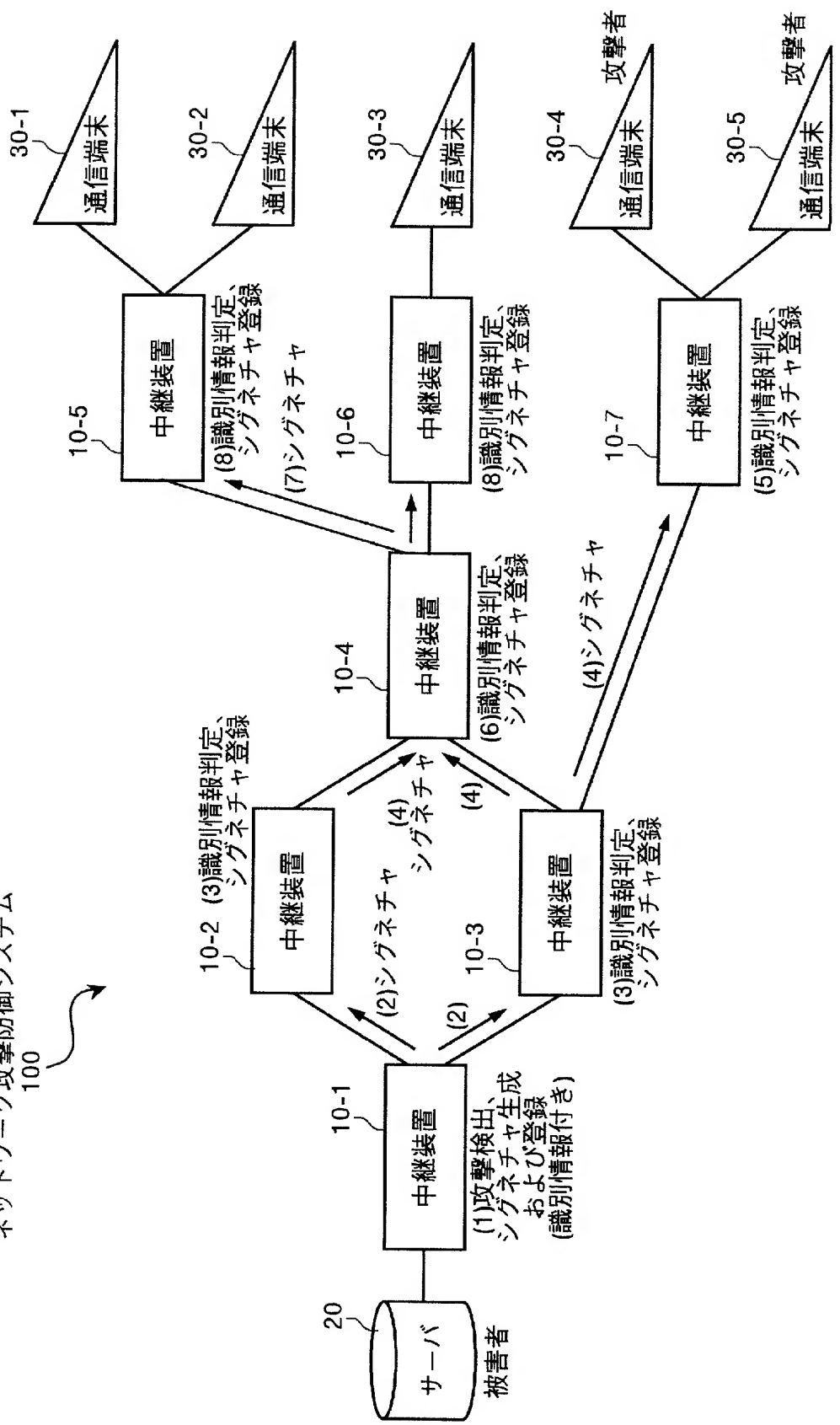
。 【図 1 3】 従来技術に係るネットワーク攻撃防御システムを説明するための図である。

【符号の説明】

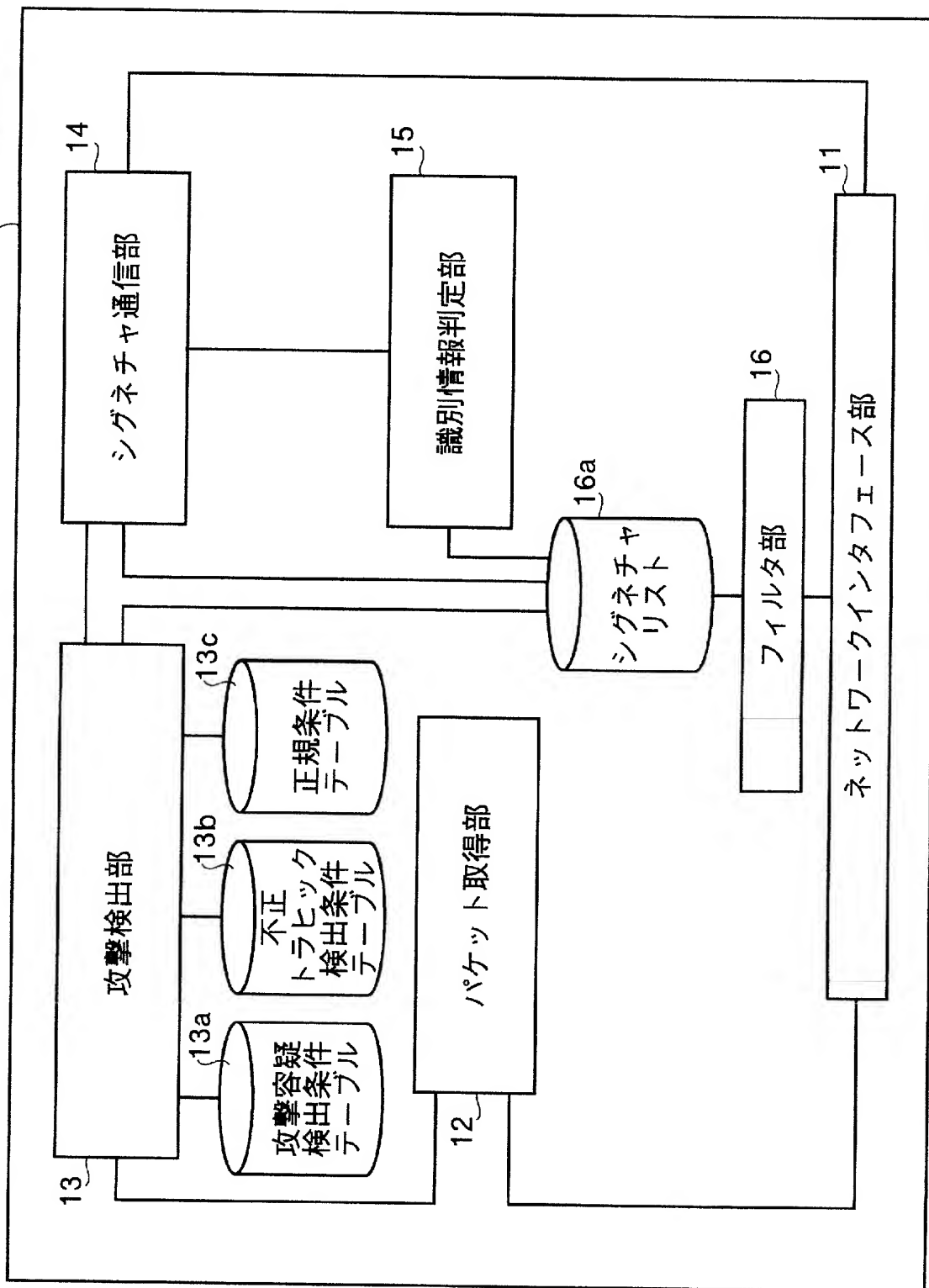
【 0 1 1 7 】

- 1 0 中継装置
- 1 1 ネットワークインタフェース
- 1 2 パケット取得部
- 1 3 攻撃検出部
- 1 4 シグネチャ通信部
- 1 5 識別情報判定部
- 1 6 フィルタ部
- 2 0 サーバ
- 3 0 通信端末
- 1 0 0 ネットワーク攻撃防御システム

ネットワーク攻撃防御システム
100



10 中継装置



13a 攻撃容疑検出条件テーブル

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500Kbps	10秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300Kbps	10秒
3	{Dst=192.168.1.1/24}	1000Kbps	20秒
⋮			

13b 不正トラヒック条件検出テーブル

番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
3	T3Kbps以上のフラグメントパケットが S3秒以上連続送信されている
⋮	

13c 正規条件テーブル

番号	検出属性
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

16a シグネチャリスト

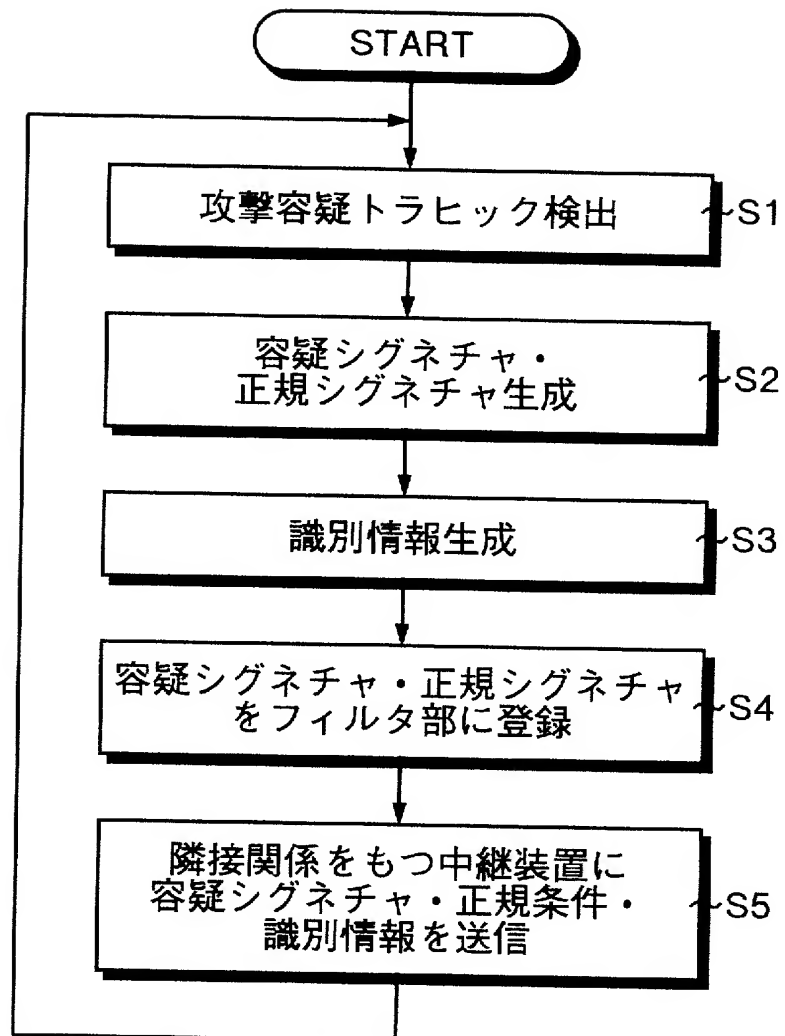


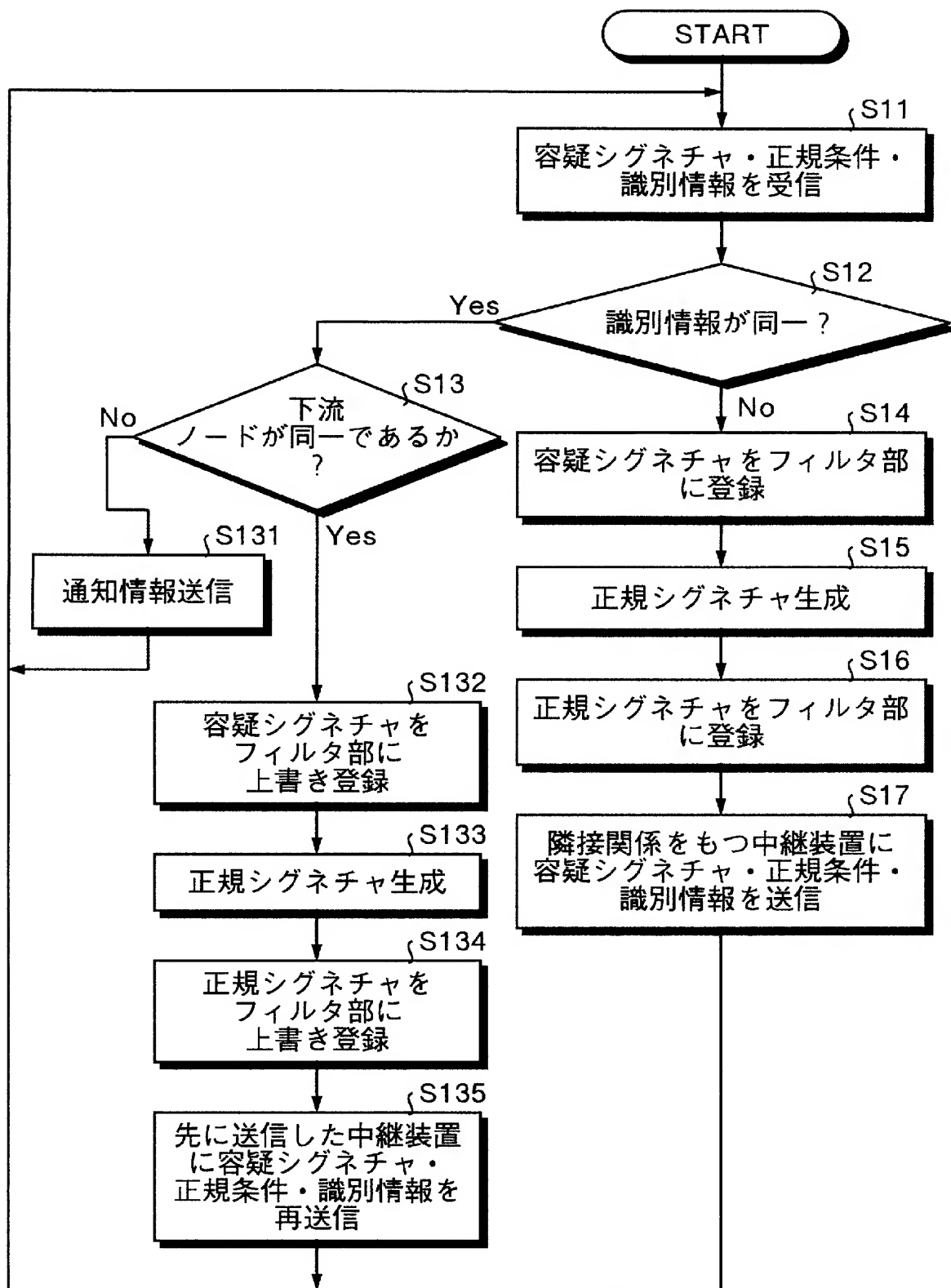
シグネチャ	識別情報	下流ノード	上流ノード
シグネチャA	(..., ..., ..., ...)	中継装置 10-2	中継装置 10-5, 10-6
シグネチャB	(..., ..., ..., ...)	中継装置 10-3	中継装置 10-5, 10-6
⋮	⋮	⋮	⋮

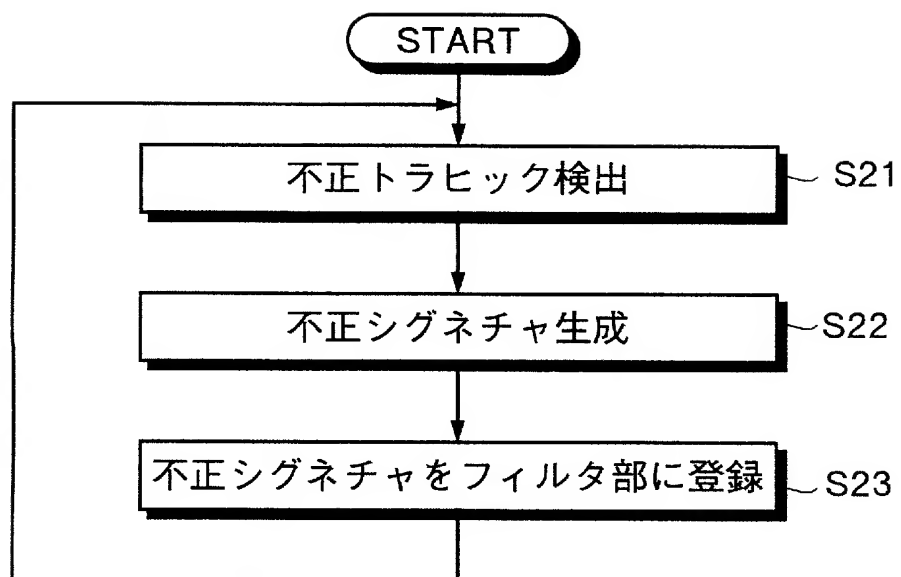
【図 7】

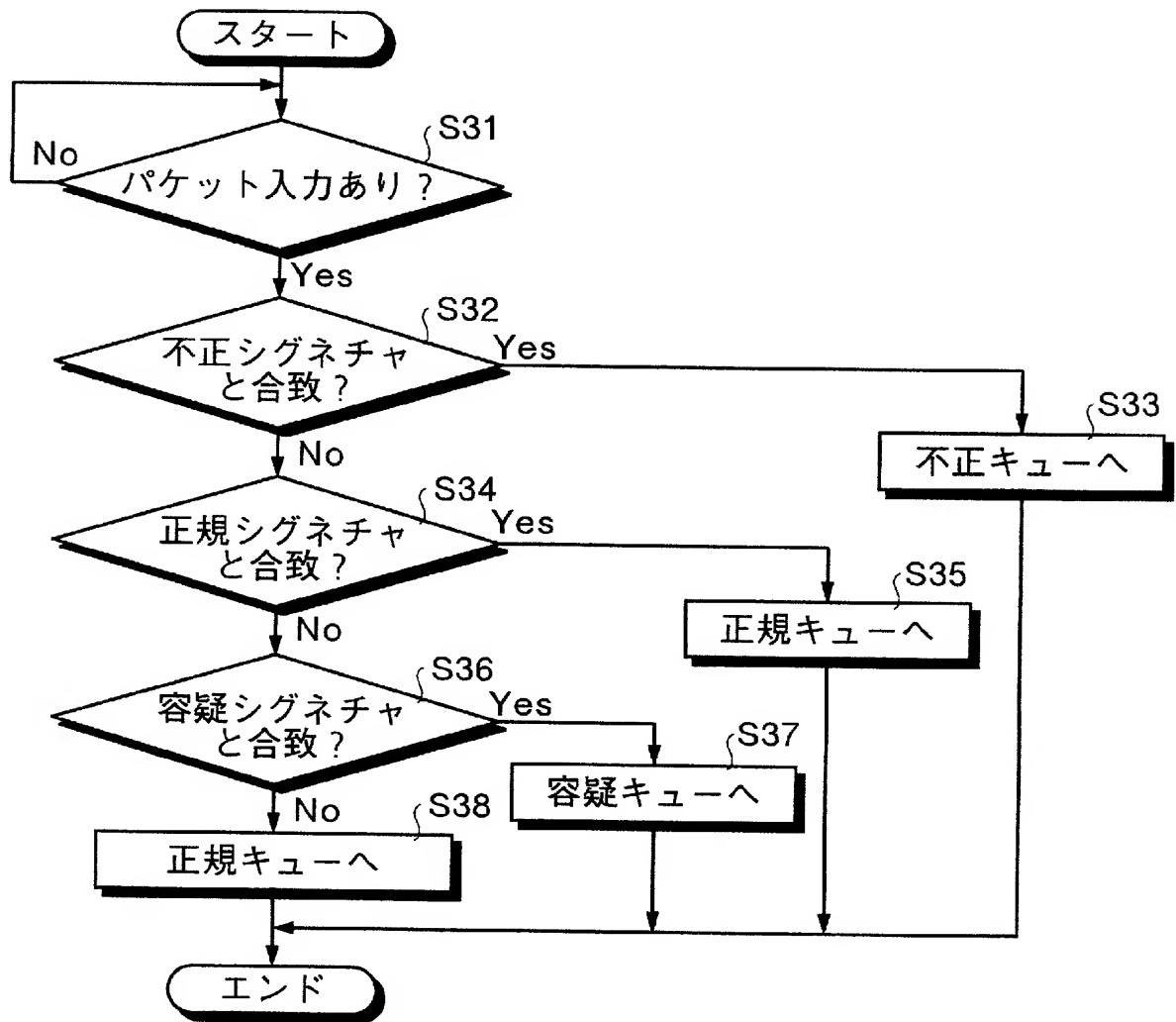
識別情報: {Local Alert ID, Engine-type, Engine-ID, Node-ID}

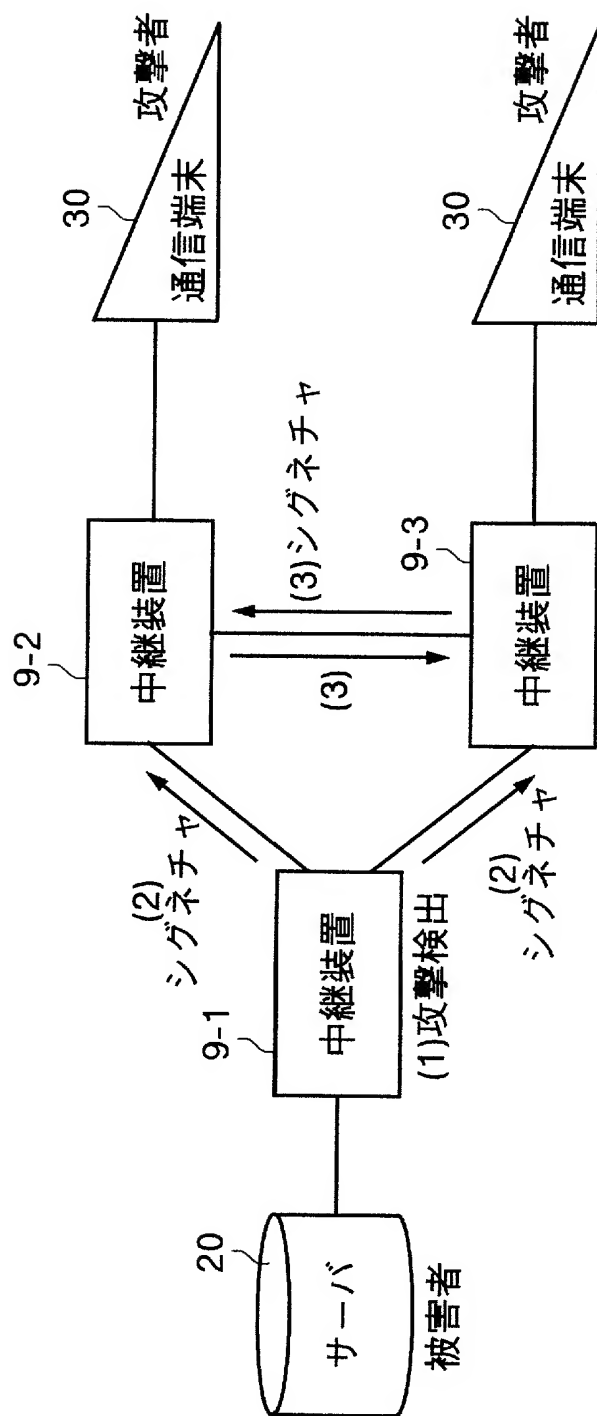
- Local Alert ID: Analysis Engine内でユニークなAlertの識別子
- Engine-type: Analysis Engineの種類の識別子
- Engine-ID: 同一Mitigationに帰属する
同種のAnalysis Engineの識別子
- Node-ID: Analysis Engineが帰属するMitigationのノード識別子

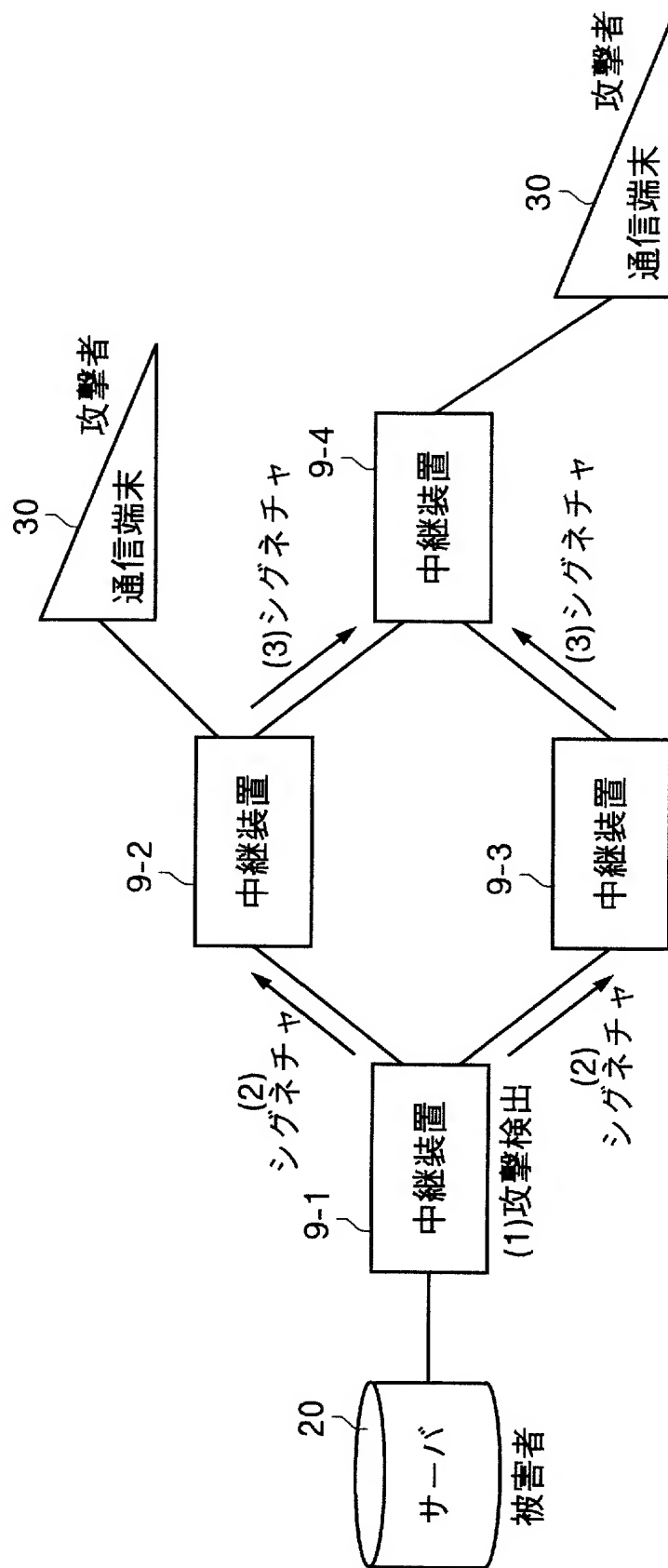












【書類名】 要約書

【要約】

【課題】 シグネチャの重複登録や重複送信を回避し、シグネチャに基づいたパケット制御を効率的に行うことを課題とする。

【解決手段】 容疑のかかる攻撃を検出した中継装置 10 では、攻撃容疑パケットを制限するための容疑シグネチャおよび容疑シグネチャの生成を一意に識別するための識別情報を生成するとともに、生成した容疑シグネチャおよび識別情報を隣接中継装置に送信する。かかる容疑シグネチャおよび識別情報を受信した中継装置 10 では、受信した容疑シグネチャの識別情報が自己のシグネチャリストに既に登録されているか否かを判定し、未だ登録されていない場合には、受信した容疑シグネチャおよび識別情報をシグネチャリストに登録するとともに、当該容疑シグネチャおよび識別情報を隣接中継装置に送信する。

【選択図】 図 1

出願人履歴

0 0 0 0 0 4 2 2 6

19990715

住所変更

5 9 1 0 2 9 2 8 6

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社